대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0047430
Application Number

출 원 년 월 일 : 2003년 07월 11일
Date of Application JUL 11, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2004 년 01 월 27 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	명세서 등 보정서
【수신처】	특허청장
【제출일자】	2004.01.10
【제출인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【사건과의 관계】	출원인
【대리인】	
【성명】	김동진
【대리인코드】	9-1999-000041-4
【포괄위임등록번호】	2002-007585-8
【사건의 표시】	
【출원번호】	10-2003-0047430
【출원일자】	2003.07.11
【발명의 명칭】	기기간 컨텐츠 교환을 위한 도메인 인증 방법
【제출원인】	
【접수번호】	1-1-2003-0254105-26
【접수일자】	2003.07.11
【보정할 서류】	명세서등
【보정할 사항】	
【보정대상항목】	별지와 같음
【보정방법】	별지와 같음
【보정내용】	별지와 같음
【취지】	특허법시행규칙 제13조·실용신안법시행규칙 제8조의 규정에의하여 위와 같 이 제출합니다. 대리인 김동진 (인)
【수수료】	
【보정료】	0 원
【추가심사청구료】	0 원
【기타 수수료】	0 원
【합계】	0 원
【첨부서류】	1. 보정내용을 증명하는 서류_1통

【보정대상항목】 요약

【보정방법】 정정

【보정내용】

본 발명은 기기간 컨텐츠 교환을 위한 도메인 인증 방법에 관한 발명으로서, 유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제1단계와, 상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제2단계와, 도메인 비밀키 보유여부를 판별하는 절차의 예로서 소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 제1패킷을 전송하는 제3단계와, 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 제1패킷으로부터 상기 1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 암호화한 제2패킷을 수신하는 제4단계, 및 상기 제2단계에서 생성한 도메인 비밀키를 이용하여 상기 제 4단계에서 수신한 제2패킷을 복호하고, 상기 복호된 제2패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제5단계를 포함하는 것을 특징으로 한다.

【보정대상항목】 식별번호 9

【보정방법】 정정

【보정내용】

또한, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 유무선 네트워크상에 포함되는 소정의 기기에 도메인

식별정보를 설정하는 제1단계와, 상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제2단계와, 도메인 비밀키 보유여부를 판별하는 절차의 예로서 소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 제1패킷을 전송하는 제3단계와, 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 제1패킷으로부터 상기 제1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 암호화한 제2패킷을 수신하는 제4단계, 및 상기 제 2단계에서 생성한 도메인 비밀키를 이용하여 상기 제 4단계에서 수신한 제2패킷을 복호하고, 상기 복호된 제2패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제5단계를 포함한다. 바람직하게는 상기 도메인 비밀키는 상기 도메인 식별정보와 상기 디바이스 식별정보를 입력변수로 하는 암호적으로 강한 일방향 함수의 결과값 또는 해쉬 함수의 결과값인 것으로 하고, 상기 제1코드값과 상기 제2코드값은 기기 자신에 의해 생성된 소정 비트의 난수인 것으로 한다.

【보정대상항목】 식별번호 10

【보정방법】 정정

【보정내용】

한편, 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 상기 제5단계에서 상기 복호된 제2패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 컨텐츠의 암호화에 사용될 세션키를 생성하고, 동일하지 않은 경우에는 도메인 인증절차를 종료

하는 단계를 더 포함한다. 또다른 실시예로로서 상기 제5단계는 상기 복호된 제2패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 상기 복호된 패킷의 다른 특정 비트프레임을 전송하는 단계를 더 포함한다.

【보정대상항목】 식별번호 11

【보정방법】 정정

【보정내용】

또한, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 디바이스 식별정보를 이용하여 디바이스 상호 인증을 수행하는 제1단계와, 유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제2단계와, 상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제3단계와, 소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 제1패킷을 전송하는 제4단계와, 상기 제 3단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 패킷으로부터 상기 제1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 3단계에서 생성된 도메인 비밀키를 이용하여 암호화한 제2패킷을 수신하는 제5단계, 및 상기 제3단계에서 생성한 도메인 비밀키를 이용하여 상기 제5단계에서 수신한 제2패킷을 복호하고, 상기 복호된 제2패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제6단계를 포함한다. 바람직하게는 상기 도메인 비밀키는 상기 도메인 식별정보와 상기 디바이스 식별정보를 입력변수로 하는 암호적으로 강한 일방향 함수의 결과값

또는 해쉬 함수의 결과값인 것으로 하고, 상기 제1코드값과 상기 제2코드값은 기기 자신에 의해 생성된 소정 비트의 난수인 것으로 한다.

【보정대상항목】 식별번호 12

【보정방법】 정정

【보정내용】

한편, 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 상기 제6단계에서 상기 복호된 제2패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값이 동일한 경우에는 컨텐츠의 암호화에 사용될 세션키를 생성하고, 동일하지 않은 경우에는 도메인 인증절차를 종료하는 단계를 더 포함한다. 또다른 실시예로로서 상기 제6단계는 상기 복호된 제2패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값이 동일한 경우에는 상기 복호된 패킷의 다른 특정 비트프레임을 전송하는 단계를 더 포함한다.

【보정대상항목】 식별번호 16

【보정방법】 정정

【보정내용】

【수학식 1】

$$K=F(DomainID,DeviceID)$$

【보정대상항목】 식별번호 17

【보정방법】 정정

【보정내용】

【수학식 2】

$K = H(DomainID \oplus H(DeviceID\_1 \,||\, ... \,||\, DeviceID\_n)$

)

【보정대상항목】 식별번호 18

【보정방법】 정정

【보정내용】

【수학식 3】

$K=H(DomainID \| DeviceID_1 \| ..... \| DeviceID_n)$

【보정대상항목】 청구항 3

【보정방법】 정정

【보정내용】

유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제1단계;

상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제2단계;

소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 제1패킷을 전송하는 제3단계;

상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 제1패킷으로부터 상기 제1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 암호화한 제2패킷을 수신하는 제4단계; 및

상기 제 2단계에서 생성한 도메인 비밀키를 이용하여 상기 제 4단계에서 수신한 제2패킷을 복호하고, 상기 복호된 제2패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제5단계를 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【보정대상항목】 청구항 4

【보정방법】 정정

【보정내용】

제3항에 있어서,

상기 도메인 비밀키는 상기 도메인 식별정보와 상기 디바이스 식별정보를 입력변수로 하는 암호적으로 강한 일방향 함수의 결과값으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【보정대상항목】 청구항 5

【보정방법】 정정

【보정내용】

제3항에 있어서,

상기 도메인 비밀키는 상기 도메인 식별정보와 상기 디바이스 식별정보를 입력변수로 하는 해쉬함수의 결과값으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【보정대상항목】 청구항 7

【보정방법】 정정

【보정내용】

제3항에 있어서,

상기 제5단계는 상기 복호된 제2패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 컨텐츠의 암호화에 사용될 세션키를 생성하고, 동일하지 않은 경우에는 도메인 인증절차를 종료하는 단계를 더 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법.

【보정대상항목】 청구항 8

【보정방법】 정정

【보정내용】

제3항에 있어서,

상기 제5단계는 상기 복호된 제2패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 상기 복호된 패킷의 다른 특정 비트프레임을 전송하는 단계를 더 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【보정대상항목】 청구항 9

【보정방법】 정정

【보정내용】

디바이스 식별정보를 이용하여 디바이스 상호 인증을 수행하는 제1단계;

유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제2단계;

상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제3단계;

소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 제1패킷을 전송하는 제4단계;

상기 제 3단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 제1패킷으로부터 상기 제1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코

드값과 상기 제2코드값을 상기 제 3단계에서 생성된 도메인 비밀키를 이용하여 암호화한 제2패킷을 수신하는 제5단계; 및

상기 제3단계에서 생성한 도메인 비밀키를 이용하여 상기 제5단계에서 수신한 제2패킷을 복호하고, 상기 복호된 제2패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제6단계를 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【보정대상항목】 청구항 10

【보정방법】 정정

【보정내용】

제9항에 있어서,

상기 도메인 비밀키는 상기 도메인 식별정보와 상기 디바이스 식별정보를 입력변수로 하는 암호적으로 강한 일방향 함수의 결과값으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【보정대상항목】 청구항 11

【보정방법】 정정

【보정내용】

제9항에 있어서,

상기 도메인 비밀키는 상기 도메인 식별정보와 상기 디바이스 식별정보를 입력변수로 하는 해쉬함수의 결과값으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【보정대상항목】 청구항 13

【보정방법】 정정

【보정내용】

제9항에 있어서,

상기 제6단계는 상기 복호된 제2패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값이 동일한 경우에는 컨텐츠의 암호화에 사용될 세션키를 생성하고, 동일하지 않은 경우에는 도메인 인증절차를 종료하는 단계를 더 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법.

【보정대상항목】 청구항 14

【보정방법】 정정

【보정내용】

제9항에 있어서,

상기 제6단계는 상기 복호된 제2패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값이 동일한 경우에는 상기 복호된 패킷의 다른 특정 비트프레임을 전송하는 단계를 더 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0001
【제출일자】	2003.07.11
【발명의 명칭】	기기간 컨텐츠 교환을 위한 도메인 인증 방법
【발명의 영문명칭】	Method for Domain Authentication for exchanging contents between devices
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	김동진
【대리인코드】	9-1999-000041-4
【포괄위임등록번호】	2002-007585-8
【발명자】	
【성명의 국문표기】	유용국
【성명의 영문표기】	YOU,Yong Kuk
【주민등록번호】	710815-1057150
【우편번호】	442-370
【주소】	경기도 수원시 팔달구 매탄동 1239-9
【국적】	KR
【발명자】	
【성명의 국문표기】	김명선
【성명의 영문표기】	KIM,Myung Sun
【주민등록번호】	700521-1478511
【우편번호】	437-722
【주소】	경기도 의왕시 삼동 우성4차아파트 다동 106호
【국적】	KR
【발명자】	
【성명의 국문표기】	최양림
【성명의 영문표기】	CHOI,Yang Lim
【주민등록번호】	710120-1830615

【우편번호】 463-830
【주소】 경기도 성남시 분당구 이매동 124 한신아파트 210-1509
【국적】 KR
【발명자】
【성명의 국문표기】 남수현
【성명의 영문표기】 NAM,Su Hyun
【주민등록번호】 740210-1405410
【우편번호】 137-062
【주소】 서울특별시 서초구 방배2동 435-26 102호
【국적】 KR
【발명자】
【성명의 국문표기】 장용진
【성명의 영문표기】 JANG,Yong Jin
【주민등록번호】 750112-1063416
【우편번호】 427-010
【주소】 경기도 과천시 중앙동 23-6
【국적】 KR
【취지】 특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 김동진 (인)
【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	1	면	1,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	0	항	0 원

【합계】 30,000 원
【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 기기간 컨텐츠 교환을 위한 도메인 인증 방법에 관한 발명으로서, 유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제1단계와, 상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제2단계와, 도메인 비밀키 보유여부를 판별하는 절차의 예로서 소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 패킷을 전송하는 제3단계와, 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 패킷으로부터 상기 1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 암호화한 패킷을 수신하는 제4단계, 및 상기 제 2단계에서 생성한 도메인 비밀키를 이용하여 상기 제 4단계에서 수신한 패킷을 복호하고, 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제5단계를 포함하는 것을 특징으로 한다.

【대표도】

도 3

【색인어】

DTCP, 도메인 인증

【명세서】

【발명의 명칭】

기기간 컨텐츠 교환을 위한 도메인 인증 방법{Method for Domain Authentication for exchanging contents between devices}

【도면의 간단한 설명】

도 1은 종래의 기기간 컨텐츠 교환 절차를 나타내는 예시도

도 2는 본 발명에 따른 도메인 인증 절차가 포함된 기기간 컨텐츠 교환 절차를 나타내는 예시도

도 3은 본 발명에 따른 기기간 도메인 인증 절차를 나타내는 예시도

도 4는 본 발명에 따른 도메인 인증 절차가 포함된 기기간 컨텐츠 교환 절차를 나타내는 일 실시예 처리 흐름도

도 5는 본 발명에 따른 기기간 도메인 인증 절차를 나타내는 일 실시예 처리 흐름도

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 서로 다른 두 기기간에 오디오/비디오(Audio/Video, 이하 'AV'라고 한다) 컨텐츠를 안전하게 전송하기 위한 프로토콜로서 히타치, 인텔, 마쓰시타, 소니, 도시바의 5개 업체에 의해 제안된 DTCP(Digital Transmission Content Protection)와 필립스에 의해 제안된 OCPS(Open Copy Protection System)가 있다. 상기 프로토콜들은 도 1에서 도시하는 바와 같이 상호인증 과정(120)과 세션키 교환 과정(130)이라는 2단계를 거쳐 기기간의 컨텐츠를 교환(140)하는 구

조로 되어 있다. 즉, 기기A(100)와 기기B(110)는 상기 상호인증 과정(120)을 통하여 서로 정당한 기기인지 여부를 확인한다. 만일, 서로 정당한 기기임이 확인되면, 컨텐츠의 암호화에 사용될 세션키를 생성하고 교환하는 상기 세션키 교환 과정(130)이 진행된다. 상기 세션키 교환 과정(130)을 통해 기기A(100)와 기기B(110)는 서로 동일한 세션키를 소유하게 된다. 기기A(100)와 기기B(110)간에 세션키 교환이 이루어지면 컨텐츠를 전송하고자 하는 기기는 기생성된 세션키를 이용하여 전송하려고 하는 컨텐츠를 암호화하여 전송하고, 상기 전송된 컨텐츠를 수신하는 기기는 기생성된 세션키로 수신한 컨텐츠를 복호화한다(140). 상기 기기간 컨텐츠 보호를 위한 프로토콜은 도 1에서 도시한 상호인증 과정(120)에서 컨텐츠를 주고 받는 기기들이 정당한 과정을 거쳐 제조된 기기인지만을 확인한다. 따라서, 어떤 사용자가 정당한 구입 절차를 거쳐 기기를 소유하였다면 얼마든지 타인의 기기에서 컨텐츠를 수신할 수 있다. 이러한 경우 AV 컨텐츠를 비롯한 가치있는 컨텐츠를 소유하고 있는 사용자는 자신이 원하지 않는 다른 사용자가 자신의 컨텐츠를 수신하는 것을 막기 어려운 문제점이 있으므로, 수신자가 정당한 수신권한을 갖고 있는지 확인할 필요가 있다.

【발명이 이루고자 하는 기술적 과제】

<7> 본 발명은 상기한 문제점을 해결하기 위해 안출된 것으로, 단일의 로컬 도메인을 식별해 주는 도메인 아이디를 확인하는 과정을 수행하여 도메인 아이디가 동일한 기기들 간에만 컨텐츠를 송수신할 수 있도록 함으로써 동일한 도메인에 속하지 않는 다른 사용자의 기기가 허가받지 않은 데이터의 송수신을 수행하지 못하도록 하는 방법을 제안한다.

【발명의 구성 및 작용】

<8> 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 단

계; 및 상기 설정된 도메인 식별정보를 이용하여 도메인 비밀키를 생성하는 단계 또는 상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 단계를 포함한다.

<9> 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제1단계와, 상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제2단계와, 도메인 비밀키 보유여부를 판별하는 절차의 예로서 소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 패킷을 전송하는 제3단계와, 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 패킷으로부터 상기 제1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 암호화한 패킷을 수신하는 제4단계, 및 상기 제 2단계에서 생성한 도메인 비밀키를 이용하여 상기 제 4단계에서 수신한 패킷을 복호하고, 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제5단계를 포함한다. 바람직하게는 상기 도메인 비밀키는 상기 도메인 식별정보와 상기 도메인 식별정보를 입력변수로 하는 암호적으로 강한 일방향 함수의 결과값 또는 해쉬 함수의 결과값인 것으로 하고, 상기 제1코드값과 상기 제2코드값은 기기 자신에 의해 생성된 소정 비트의 난수인 것으로 한다.

<10> 한편, 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 상기 제5단계에서 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 컨텐츠의 암호화에 사용될 세션키를 생성하고, 동일하지 않은 경우에는 도메인 인증절차를 종료하는 단계를 더 포함한다. 또다른

실시예로로서 상기 제5단계는 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 상기 복호된 패킷의 다른 특정 비트프레임을 전송하는 단계를 더 포함한다.

<11> 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 디바이스 식별정보를 이용하여 디바이스 상호 인증을 수행하는 제1단계와, 유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제2단계와, 상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제3단계와, 소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 패킷을 전송하는 제4단계와, 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 패킷으로부터 상기 제1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 암호화한 패킷을 수신하는 제5단계, 및 상기 제3단계에서 생성한 도메인 비밀키를 이용하여 상기 제5단계에서 수신한 패킷을 복호하고, 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제6단계를 포함한다. 바람직하게는 상기 도메인 비밀키는 상기 도메인 식별정보와 상기 도메인 식별정보를 입력변수로 하는 암호적으로 강한 일방향 함수의 결과값 또는 해쉬 함수의 결과값인 것으로 하고, 상기 제1코드값과 상기 제2코드값은 기기 자신에 의해 생성된 소정 비트의 난수인 것으로 한다.

<12> 한편, 또한, 상기 목적을 달성하기 위하여, 본 발명의 실시에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법은 상기 제6단계에서 상기 복호된 패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값이 동일한 경우에는 컨텐츠의 암호화에 사용될 세션키를 생성하고, 동일하지 않은 경우에는 도메인 인증절차를 종료하는 단계를 더 포함한다. 또다른

실시예로로서 상기 제5단계는 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 상기 복호된 패킷의 다른 특정 비트프레임을 전송하는 단계를 더 포함한다.

<13> 이하, 첨부된 도면을 참조하여 본 발명의 일 실시예에 따른 기기간 컨텐츠 교환을 위한 도메인 인증 방법을 설명하면 다음과 같다.

<14> 도 2는 본 발명에 따른 도메인 인증 절차가 포함된 기기간 컨텐츠 교환 절차를 나타내는 예시도로서, 기기A(200)와 기기B(210)는 상기 상호인증 과정을 통하여 서로 정당한 기기인지 여부를 확인한다(220). 만일, 서로 정당한 기기임이 확인되면, 상호간에 동일한 도메인 아이디를 갖고 있는지 여부를 확인하는 절차를 수행한다(225). 만일 상기 기기A(200)와 상기 기기B(210)가 서로 동일한 도메인 아이디를 갖고 있음이 확인되면 컨텐츠의 암호화에 사용될 세션키를 생성하고 교환하는 세션키 교환 과정(230)이 진행된다. 상기 세션키 교환 과정(230)을 통해 기기A(200)와 기기B(210)는 서로 동일한 세션키를 소유하게 된다. 상기 기기A(200)와 상기 기기B(210)간에 세션키 교환이 이루어지면 컨텐츠를 전송하고자 하는 기기는 기생성된 세션키를 이용하여 전송하려고 하는 컨텐츠를 암호화하여 전송하고, 상기 전송된 컨텐츠를 수신하는 기기는 기생성된 세션키로 수신한 컨텐츠를 복호화한다(240).

<15> 도 3은 본 발명에 따른 기기간 도메인 인증 절차를 나타내는 예시도로서, 상기 도 2에서 도시한 도메인 인증 절차(225)를 구체적으로 설명하고 있다. 우선, 특정한 단일의 로컬 도메인에 속하는 각각의 기기는 도메인 식별자(Domain Identifier, 이하 'DomainID'라고 한다)와 상기 DomainID에 의해 구별되는 도메인에 속하는 n개의 기기들에 대한 각각의 식별자(Device Identifier, 이하 'DeviceID'이라 한다)에 대한 정보가 설정되어야 한다. 이 때, 상기 DomainID는 특정 네트워크를 관리하는 관리자가 해당 기기에 직접 입력하거나, 상기 특정 네트

워크를 관리하는 서버에서 자동적으로 생성하여 관리할 수도 있다. 또한, 상기 DeviceID은 일반적으로 MAC 주소로 할 수 있다. 데이터를 송수신하고자 하는 기기A(300)와 기기B(310)는 도메인을 결성할 n개의 기기 식별자를 나타내는 DeviceID_1, DevcieID_2, ..., DeviceID_n를 입력변수로 하여 DeviceID를 생성하고, 상기 생성된 DeviceID 또는 기저장된 DomainID를 입력변수로 하여 비밀값을 생성한다(312,314). 즉, 상기 비밀키를 K라고 하고, 암호적으로 강한 일방향함수를 F라고 한다면, 상기 비밀키 K는 [수학식 1] 내지 [수학식 4]과 같은 방법으로 나타낼 수 있다. 이 때, 함수 H는 해쉬함수를 나타낸다.

<16> 【수학식 1】 K = F(DomainID, DeviceID)

<17> 【수학식 2】 K = H(DomainID $\oplus$ H(DeviceID_1 || ..... || DeviceID_n)

)

<18> 【수학식 3】 K = H(DomainID || DeviceID_1 || ..... || DeviceID_n)

<19> K = H(DomainID || H(DeviceID_1 || ..... || DeviceID_n))

<20> 【수학식 4】 K = DomainID

<21> 이 때, 소정의 값 A, B에 대하여 'A || B'는 A값과 B값의 나열을 의미한다. 상기 기기A(300)와 상기 기기B(310)가 상기 동일한 비밀키 K를 생성한 후, 만일 상기 기기A(300)가 상기 기기B(310)로부터 소정의 컨텐츠를 수신하고자 한다면, 여러가지 방식으로 비밀키 K의 보유여부를 확인할 수 있는데 그 한가지 방법을 예시해본다. 상기 기기A(300)는 랜덤하게 난수 r_1를 생성하고, 상기 생성된 난수는 대칭암

호화 함수 E에 의하여 상기 비밀키 K로 암호화된다(316). 이 때, 암호화된 값을 $E_k(r_1)$라고 하면, 상기 기기A(300)는 상기 $E_k(r_1)$를 상기 기기B(310)로 전송한다(318). 한편, 기기B(310)는 기생성된 비밀키 K를 이용하여 상기 기기A(300)로부터 수신한 $E_k(r_1)$를 복호화함으로써 r_1'값을 얻는다(320). 그리고 나서, 상기 기기B(310)는 난수 r_2를 생성하고 r_2와 r_1'는 상기 대칭암호화 함수 E에 의하여 상기 비밀키 K로 함께 암호화된다(322). 이 때, 암호화된 값을 $E_k(r_1'||r_2)$라고 하면, 상기 기기B(310)는 상기 $E_k(r_1'||r_2)$를 상기 기기A(300)로 전송한다(324). 상기 기기A(300)는 비밀키 K를 이용하여 상기 기기B(310)로부터 수신한 $E_k(r_1'||r_2)$를 복호화함으로써 $r_1'||r_2'$ 값을 얻고, 여기에서 r_1'이 자신이 기생성한 랜덤수 r_1 와 같음을 확인한다(326). 만일 같다면 상기 기기A(300)는 r_2'을 상기 기기B(310)에게 전송하고(328), 상기 기기B(310)는 상기 수신한 r_2'가 자신이 기생성한 랜덤수 r_2와 같음을 확인한다(330). 이와 같은 방법으로 기기A(300)와 기기B(310)는 서로 동일한 도메인에 속한 기기임을 확인할 수 있고, 만일 동일한 도메인에 속한 기기들이라면 상기 도 2에서 도시한 세션키 교환 절차(230)를 수행하게 된다. 한편, 상기 '326'과정, 상기 '330'과정에 있어서 자신이 기생성한 랜덤수와 동일하지 않음이 확인되면, 상기 도메인 인증 절차는 중단되고 도메인 인증실패 메시지를 생성하여 각각의 기기 사용자에게 제공한다.

<22> 도 4는 본 발명에 따른 도메인 인증 절차가 포함된 기기간 컨텐츠 교환 절차를 나타내는 일 실시예 처리 흐름도로서, 컨텐츠를 송수신하고자 하는 각각의 기기는 자신의 인증서를 상대방에게 전송(S405)하고, 수신한 상대방의 인증서를 확인한여(S410), 상기 수신한 인증서가 유효한지 여부를 검사한다(S415). 만일 유효한 인증서가 아니라면 인증절차는 종료되고(S435), 유효한 인증서라면, 각각의 기기가 서로 동일한 도메인 아이디를 갖고 있는지 여부를 검사한다(S420). 만일 서로 동일한 아이디를 갖고 있지 않다면 인증절차는 종료되고(S435), 동일한 도

메인 아이디를 갖고 있다면 각각의 기기는 세션키를 생성하고 이를 교환한 후(S425), 상기 세션키로 암호화된 컨텐츠를 교환하게 된다(S430).

<23> 도 5는 본 발명에 따른 기기간 도메인 인증 절차를 나타내는 일 실시예 처리 흐름도로서, 만일 컨텐츠를 송수신하기 위한 기기A와 기기B가 존재하고, 상기 기기A가 상기 기기B로부터 소정의 컨텐츠를 수신하고자 하면, 상기 기기간의 기기 인증 절차를 거친 후, 상기 도 5에서 도시한 도메인 인증절차를 거치게 된다. 상기 기기A와 상기 기기B는 자신의 비밀키 K값을 생성한 후(S505), 상기 기기A는 난수 r_1을 발생시키고 상기 비밀키 K값을 이용하여 상기 r_1을 암호화하고 상기 기기B에게 상기 암호화된 r_1값, 즉 $E_k(r_1)$ 값을 전달한다(S510). 상기 기기B는 수신한 $E_k(r_1)$ 값으로부터 r_1'을 계산하고(S515), 난수 r_2를 발생시키고 상기 비밀키 K값을 이용하여 상기 r_1'와 r_2을 함께 암호화하고 상기 기기A에게 상기 암호화된 값, 즉 $E_k(r_1'||r_2)$ 값을 전달한다(S520). 상기 기기A는 수신한 $E_k(r_1'||r_2)$ 값을 복호하여 r_1'을 추출하고(S525), 자신이 기생성한 랜덤수 r_1와 동일한지 여부를 검사한다(S530). 만일 동일하지 않으면 도메인 인증절차는 종료되고(S550), 동일하면 상기 기기A가 $E_k(r_1'||r_2)$ 값을 복호하여 추출한 r_2'를 상기 기기B에게 전달한다(S535). 상기 기기B는 상기 수신한 r_2'가 자신이 기생성한 랜덤수 r_2와 동일하지 여부를 검사하고(S540), 만일 동일하지 않으면 도메인 인증절차는 종료되고(S550), 동일하면 세션키 교환 절차를 진행하게 된다(S545).

<24> 이상에서 설명한 본 발명은, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 있어 본 발명의 기술적 사상을 벗어나지 않는 범위 내에서 여러 가지 치환, 변형 및 변경이 가능하므로 전술한 실시예 및 첨부된 도면에 한정하는 것은 아니다.

【발명의 효과】

<25> 상기한 바와 같이 이루어진 본 발명에 따르면, 종래의 기기나 컨텐츠 보호를 위한 프로토콜에 도메인 아이디 인증 절차를 추가함으로써 다른 도메인에 속하는 사용자가 허락없이 컨텐츠를 송수신할 수 없도록 하여 안전한 컨텐츠 교환을 수행할 수 있다.

【특허청구범위】

【청구항 1】

유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 단계; 및

상기 설정된 도메인 식별정보를 이용하여 도메인 비밀키를 생성하는 단계를 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 2】

유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 단계; 및

상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 단계를 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 3】

유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제1단계;

상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제2단계;

소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 패킷을 전송하는 제3단계;

상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 패킷으로부터 상기 제1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 암호화한 패킷을 수신하는 제4단계; 및

상기 제 2단계에서 생성한 도메인 비밀키를 이용하여 상기 제 4단계에서 수신한 패킷을 복호하고, 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제5단계를 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 4】

제3항에 있어서,

상기 도메인 비밀키는 상기 도메인 식별정보와 상기 도메인 식별정보를 입력변수로 하는 암호적으로 강한 일방향 함수의 결과값으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 5】

제3항에 있어서,

상기 도메인 비밀키는 상기 도메인 식별정보와 상기 도메인 식별정보를 입력변수로 하는 해쉬함수의 결과값으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 6】

제3항에 있어서,

상기 제1코드값과 상기 제2코드값은 기기 자신에 의해 생성된 소정 비트의 난수인 것으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증 방법

【청구항 7】

제3항에 있어서,

상기 제5단계는 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 컨텐츠의 암호화에 사용될 세션키를 생성하고, 동일하지 않은

경우에는 도메인 인증절차를 종료하는 단계를 더 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법.

【청구항 8】

제3항에 있어서,

상기 제5단계는 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값이 동일한 경우에는 상기 복호된 패킷의 다른 특정 비트프레임을 전송하는 단계를 더 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 9】

디바이스 식별정보를 이용하여 디바이스 상호 인증을 수행하는 제1단계;

유무선 네트워크상에 포함되는 소정의 기기에 도메인 식별정보를 설정하는 제2단계;

상기 설정된 도메인 식별정보와 소정의 디바이스 식별정보를 이용하여 도메인 비밀키를 생성하는 제3단계;

소정의 제1코드값을 생성하고 상기 제2단계에서 생성된 도메인 비밀키를 이용하여 상기 제1코드값을 암호화한 패킷을 전송하는 제4단계;

상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 상기 암호화된 패킷으로부터 상기 제1코드값을 복호하고, 소정의 제2코드값을 생성하여 상기 복호된 제1코드값과 상기 제2코드값을 상기 제 2단계에서 생성된 도메인 비밀키를 이용하여 암호화한 패킷을 수신하는 제5단계; 및

상기 제3단계에서 생성한 도메인 비밀키를 이용하여 상기 제5단계에서 수신한 패킷을 복호하고, 상기 복호된 패킷의 특정 비트프레임과 상기 제3단계에서 생성한 소정의 제1코드값과 동일한지 여부를 판단하는 제6단계를 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 10】

제9항에 있어서,

상기 도메인 비밀키는 상기 도메인 식별정보와 상기 도메인 식별정보를 입력변수로 하는 암호적으로 강한 일방향 함수의 결과값으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 11】

제9항에 있어서,

상기 도메인 비밀키는 상기 도메인 식별정보와 상기 도메인 식별정보를 입력변수로 하는 해쉬함수의 결과값으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【청구항 12】

제9항에 있어서,

상기 제1코드값과 상기 제2코드값은 기기 자신에 의해 생성된 소정 비트의 난수인 것으로 하는 기기간 컨텐츠 교환을 위한 도메인 인증 방법

【청구항 13】

제9항에 있어서,

상기 제6단계는 상기 복호된 패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값이 동일한 경우에는 컨텐츠의 암호화에 사용될 세션키를 생성하고, 동일하지 않은

경우에는 도메인 인증절차를 종료하는 단계를 더 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법.

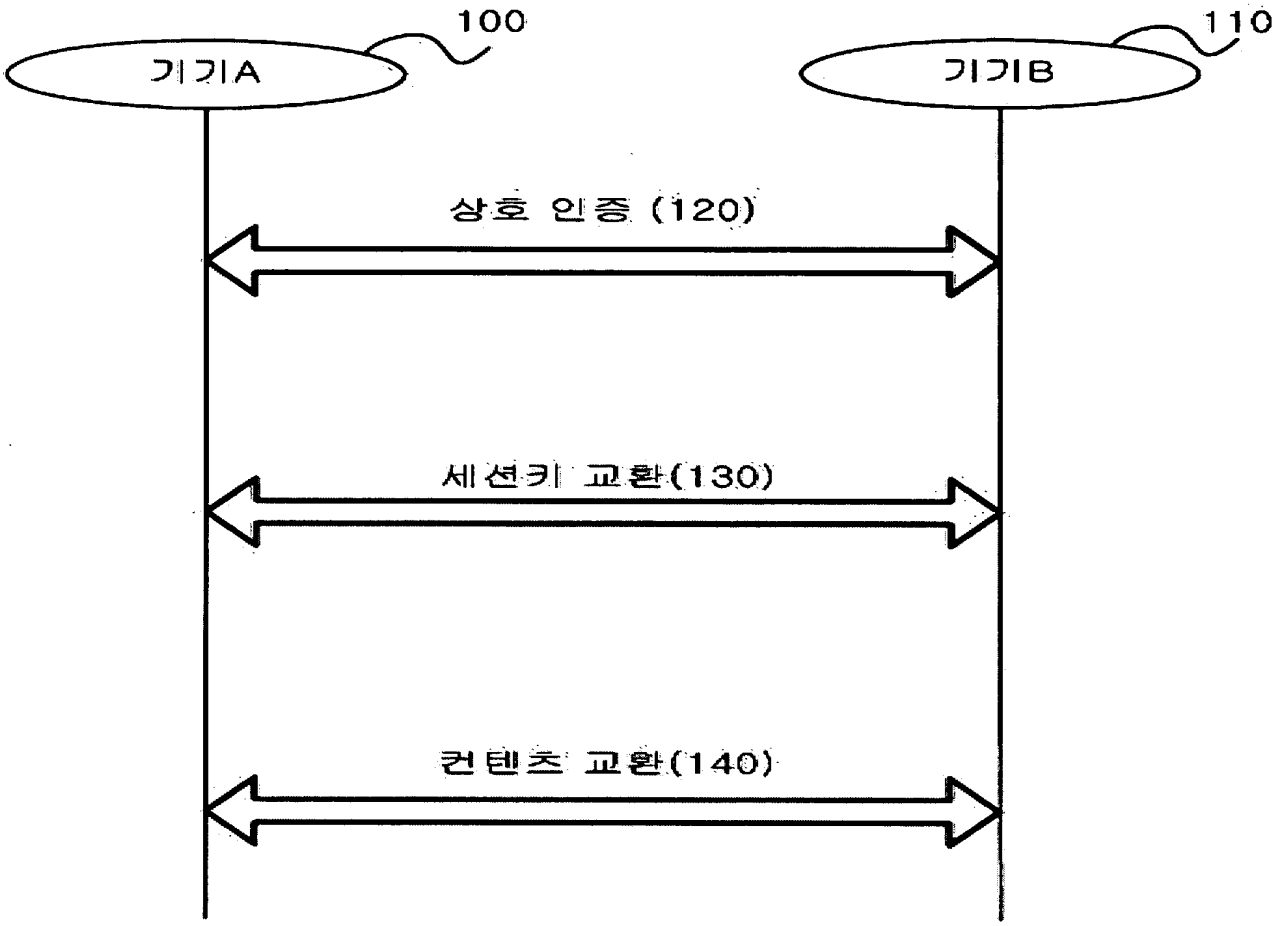
【청구항 14】

제9항에 있어서,

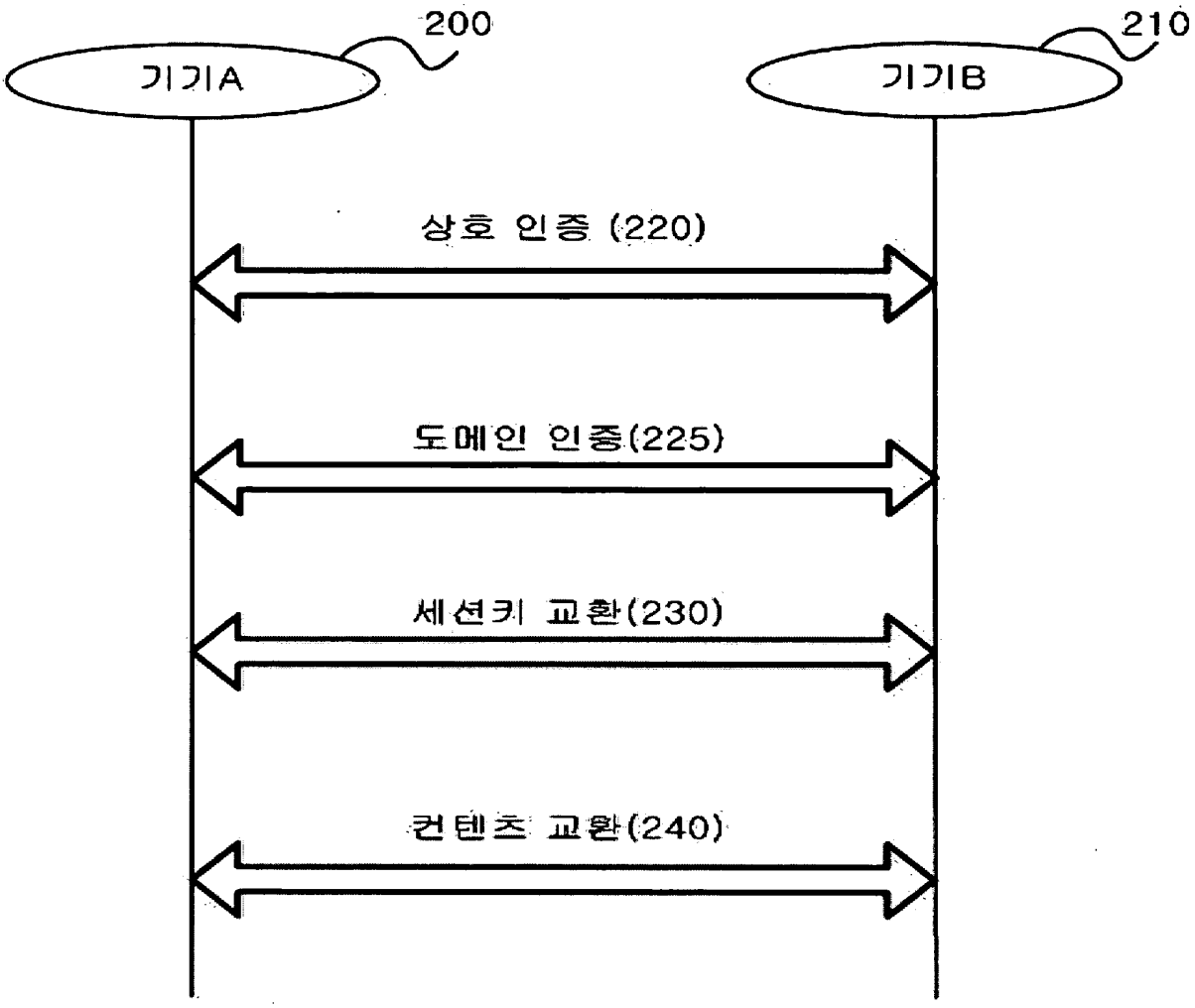
상기 제6단계는 상기 복호된 패킷의 특정 비트프레임과 상기 제4단계에서 생성한 소정의 제1코드값이 동일한 경우에는 상기 복호된 패킷의 다른 특정 비트프레임을 전송하는 단계를 더 포함하는 기기간 컨텐츠 교환을 위한 도메인 인증방법

【도면】

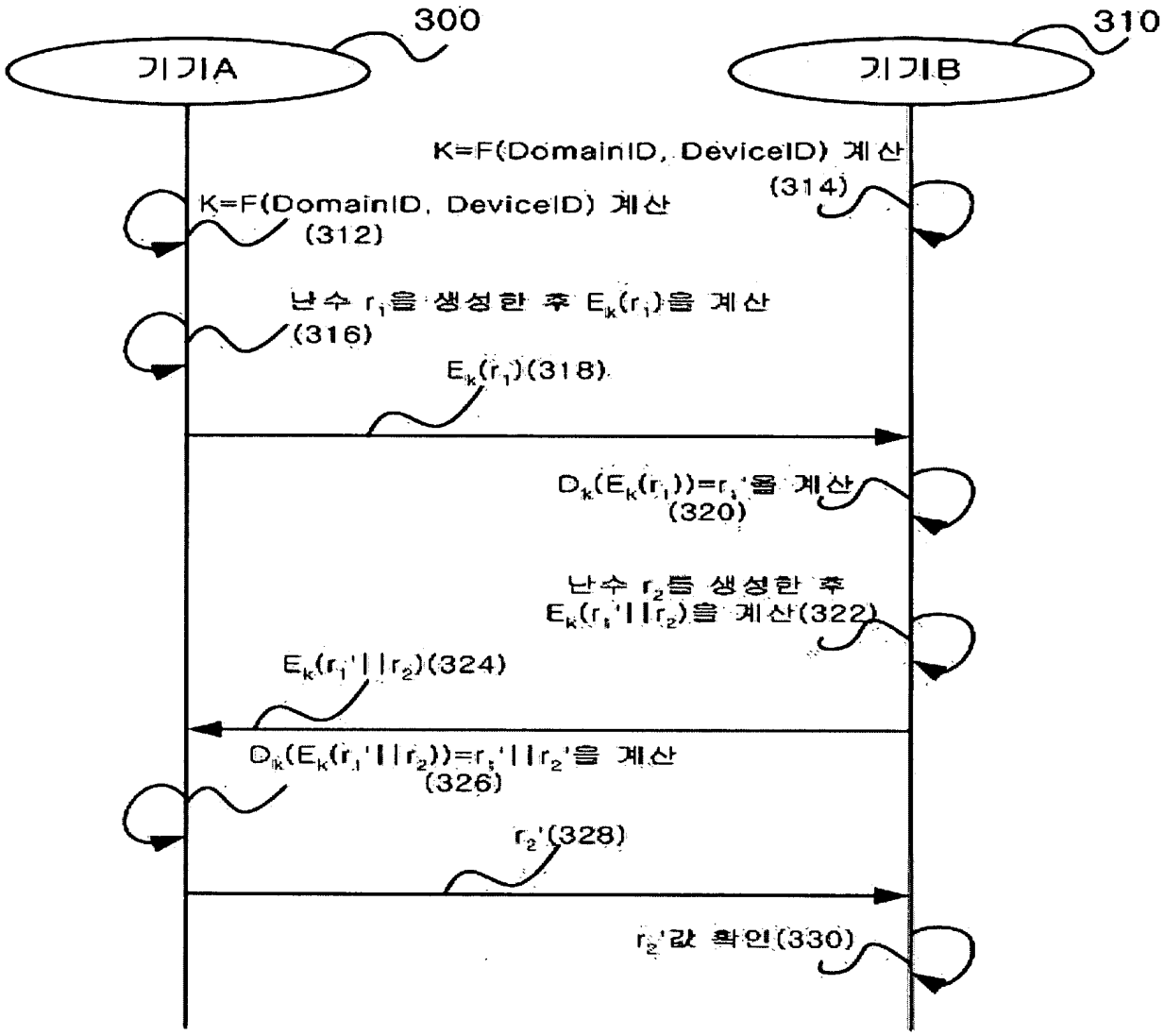
【도 1】



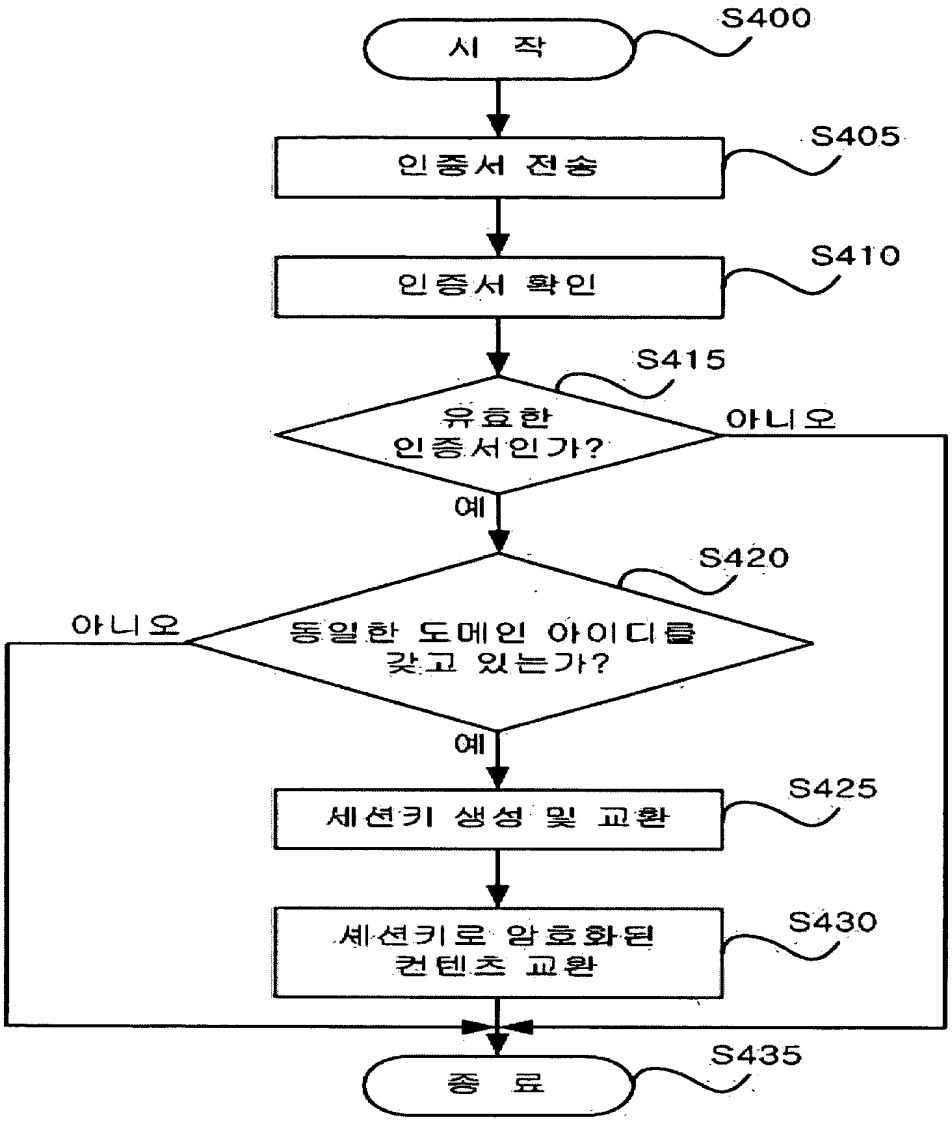
【도 2】



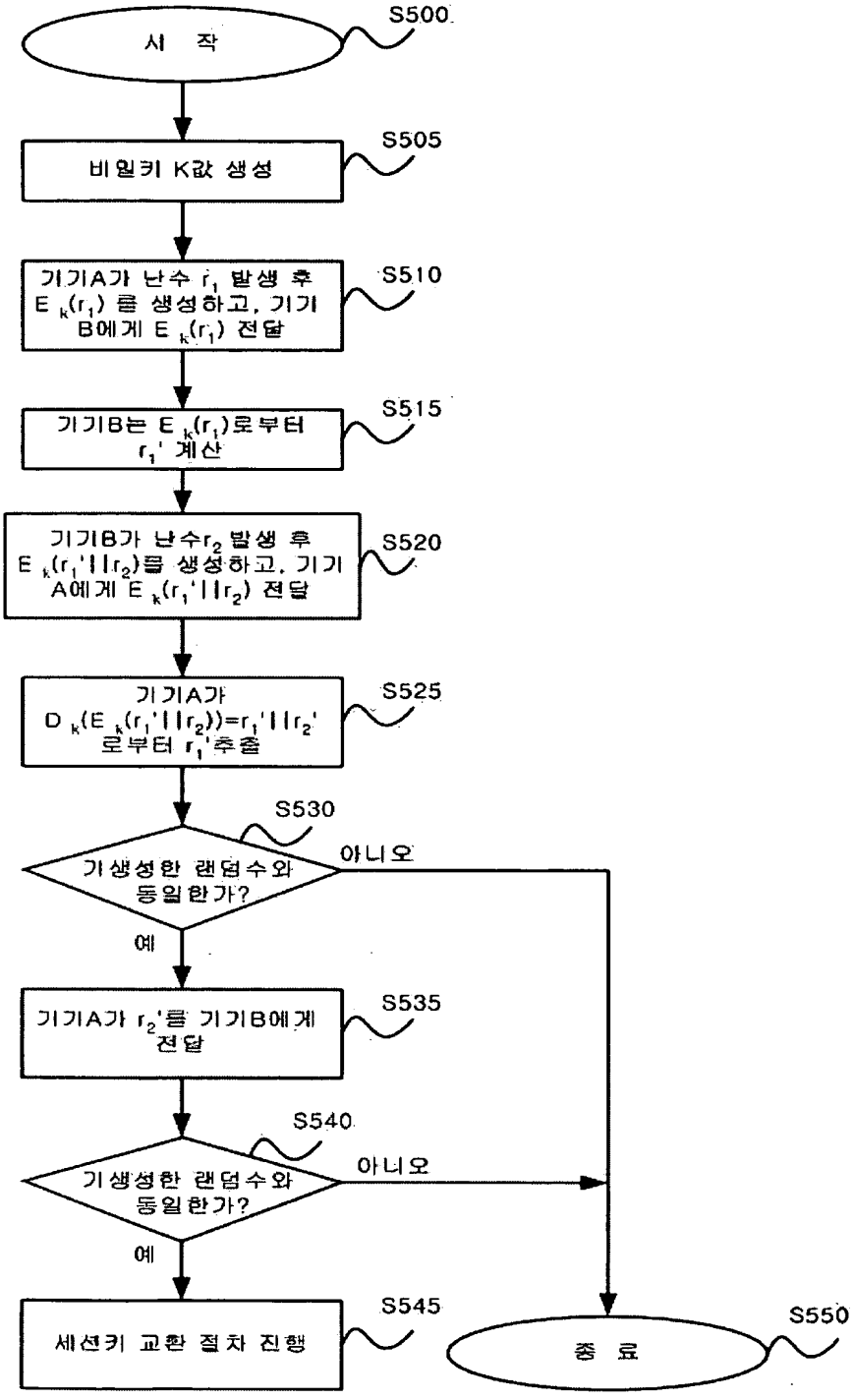
【도 3】


300
310
기기A
기기B
K=F(DomainID, DeviceID) 계산 (314)
K=F(DomainID, DeviceID) 계산 (312)
난수 r_1을 생성한 후 $E_k(r_1)$을 계산 (316)
$E_k(r_1)$(318)
$D_k(E_k(r_1))=r_1'$을 계산 (320)
난수 r_2를 생성한 후 $E_k(r_1'||r_2)$을 계산(322)
$E_k(r_1'||r_2)$(324)
$D_k(E_k(r_1'||r_2))=r_1'||r_2'$을 계산 (326)
r_2'(328)
r_2'값 확인(330)

【도 4】


S400
시 작
S405
인증서 전송
S410
인증서 확인
S415
유효한
인증서인가?
아니오
예
S420
동일한 도메인 아이디를
갖고 있는가?
아니오
예
S425
세션키 생성 및 교환
S430
세션키로 암호화된
컨텐츠 교환
S435
종 료

【도 5】


시 작
S500
비밀키 K값 생성
S505
기기A가 난수 r_1 발생 후 $E_k(r_1)$ 를 생성하고, 기기 B에게 $E_k(r_1)$ 전달
S510
기기B는 $E_k(r_1)$로부터 r_1' 계산
S515
기기B가 난수r_2 발생 후 $E_k(r_1'||r_2)$를 생성하고, 기기 A에게 $E_k(r_1'||r_2)$ 전달
S520
기기A가 $D_k(E_k(r_1'||r_2))=r_1'||r_2'$ 로부터 r_1'추출
S525
S530
기생성한 랜덤수와 동일한가?
아니오
예
기기A가 r_2'를 기기B에게 전달
S535
S540
기생성한 랜덤수와 동일한가?
아니오
예
세션키 교환 절차 진행
S545
종 료
S550